1. **INTRODUCTION**

Virtual Private Networks (VPNs) have emerged as a key element to maintaining internet security and anonymity in an increasingly networked society. With the rapid development of cyber-attacks and the need for safe communication links, VPNs offer a reliable way to protect internet traffic with encryption and mask users' identities. However, the effectiveness of VPNs in ensuring security and privacy is not absolute, given that vulnerabilities could stem from differences in technologies, protocols, and implementations. Such diversity necessitates rigorous testing approaches to effectively measure VPN reliability and security.

This research paper focuses on a rigorous assessment of VPN security using advanced machine learning and deep learning models. The primary objective is to predict the security of VPN IP addresses by identifying potential vulnerabilities like IP address leaks, DNS leaks, crypto weaknesses, and VPN behavioral anomalies. Traditional testing methods often have difficulty detecting faint, complex patterns that may indicate security vulnerabilities. In contrast, deep learning algorithms are good at processing large datasets and detecting latent anomalies that may compromise VPN integrity.

To achieve this, we use state-of-the-art models, namely Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU), that are best suited for handling sequential data and detecting anomalies in VPN activity. These models enable a robust VPN security evaluation framework by analyzing patterns that could represent threats. One of the key features of this research is the comparison of these algorithms, with a view to determining the best approach to enabling VPN security and privacy.[2]

Key variables including Accuracy Percentage, Mean Squared Error (MSE), and R-Squared (R²) are used in this study to measure performance. These measurements offer a thorough evaluation of algorithm performance, which aids in determining how well different VPN security mechanisms work. While MSE quantifies the discrepancy between expected and actual values, guaranteeing minimal divergence, accuracy percentage assesses how accurate predictions are. R2 is an important metric for evaluating the dependability of security algorithms since it also assesses the model's capacity to explain data variance. The study provides an organized method for assessing VPN security features by utilizing these criteria, guaranteeing that customers and developers may make well-informed VPN selections.

The results of this study provide important information about how to choose and use safe VPN systems. This research helps to improve VPN security by lowering vulnerabilities and improving online privacy by improving security evaluation techniques. These insights can help developers increase data protection measures, enhance authentication methods, and optimize encryption algorithms. By reducing the risks connected with cyber-attacks, our research helps VPN users select services that offer strong protection. The development of a safer and more secure digital environment for all users is ultimately supported by this effort, which advances security assessment techniques.

By conducting this research, we aspire to bridge the divide between traditional VPN security assessments and modern AI-based methods, obtaining a deeper understanding of vulnerabilities in VPNs and bolstering security measures for the future.[2][3]

1. **LITERATURE REVIEW**

Foundations of VPN Technology and Security: The foundations of VPN technology, including encryption standards (AES, RSA) and tunneling protocols (PPTP, L2TP, IPSec, OpenVPN), are covered in this section. Reviewing research that point to typical vulnerabilities in VPN implementations, it focuses on cryptographic flaws as well as IP and DNS leaks. Citation: W. Stallings (2016). Principles and Practice of Cryptography and Network Security. I. Goldberg; Pearson (2014). Internet privacy-enhancing technologies. Computing Surveys (CSUR), 35(1), 7–11[4][5].

An overview of machine learning and deep learning algorithms' applications in network security, including malware analysis, anomaly detection, and intrusion detection: In this section. It analyses the merits and demerits of the Random Forest, SVM, GRU, and LSTM algorithms for identifying network abnormalities. Sommer and Paxson (2010) are the authors of the reference. Outside of the closed world: On network intrusion detection with machine learning. IEEE Symposium on Security and Privacy, 2010 (pp. 305–316). IEEE; Zeydan, E., & Oğuz, Y. (2020). An overview of machine learning methods in cognitive radios. IEEE Communications Surveys & Tutorials, 20(2), 1286–1321[6].

Performance Metrics and Comparative research: This section includes research that use metrics like accuracy, precision, and recall to compare different machine learning and deep learning algorithms in security settings. For assessing model performance, it goes over the significance of evaluation measures and how to calculate them, including accuracy, Mean Squared Error (MSE), and R-squared (R^2). Al-Rajab, M., Abu Al-Haija, Q., and Al-Shawabkeh, M. (2018) are cited. Machine learning techniques for intrusion detection systems are assessed. The 17th International Conference on Computer and Information Science (ICIS), 2018 IEEE/ACIS (pp. 641-646). Shah, M., and Japkowicz, N. (2011) in IEEE. Assessing Learning Algorithms from a Classification Angle. Cambridge University Press [7][8].

Case Studies and Real-World Applications: The practical consequences and outcomes of VPN security evaluations utilizing sophisticated algorithms are highlighted in this section's case studies. The integration of machine learning and deep learning techniques by commercial VPN providers to improve security features and foster user confidence is examined. Singh, M., & Singh, S. (2017) is the source. A case study on VPN leak detection and prevention. Proceedings of the International Conference on Electronic Enterprise and Smart Computing, pp. 1–5. Choudhury, M., and Roy, K. (2020); IEEE. A survey on machine learning for security in business virtual private networks. Network and Computer Applications Journal, 150, 102487[9][10].

1. **METHODOLOGY**

To achieve the objectives set forth in this work, a systematic and organized approach was followed, including data collection, pre-processing, model training, and testing. This approach ensures a comprehensive assessment of VPN security by deep learning models. The approach is discussed below:

* **Data Gathering:** A comprehensive synthetic dataset was collected, incorporating VPN IP addresses, DNS queries, encryption methods, and behavior logs. Public VPN databases, cybersecurity threat intelligence, and monitored network environments were used as sources, where VPN usage was studied in terms of leak tests and encryption strength measurements. The dataset was enriched with secure and insecure VPN samples to enhance the quality of model training and evaluation. This step ensures the representation of varied data, amplifying the model's ability to identify anomalies in VPN behavior.
* **Pre-processing:** Pre-processing was essential to ensuring the raw dataset was accurate, consistent, and suitable for analysis. First, the data has to be cleaned up by detecting and eliminating inconsistencies such duplicate entries, incorrect values, and formatting errors. Imputation techniques were used to handle missing values in a methodical manner in order to preserve the dataset's integrity and avoid data loss. Additionally, formats were standardized through the use of normalization, guaranteeing consistency across various data sources. These procedures made it possible to produce a structured dataset that was useful for evaluating VPN security.

VPN-related activity logs were arranged into sequential data to improve the dataset's analytical utility. This allowed for the capture of temporal trends that are crucial for identifying security issues. This change made it possible to have a more thorough grasp of VPN usage patterns and any weaknesses over time. To extract useful indications of VPN security, including traffic abnormalities, encryption strength, authentication approaches, and protocol efficiency, feature engineering techniques were used. The dataset became more informative by extracting these pertinent features, which made it possible to create reliable models for assessing and enhancing VPN security measures.

* **Model Training:** Two deep learning models, Gated Recurrent Units (GRU) and Long Short-Term Memory (LSTM), were trained to determine whether a VPN IP address is secure. Hyperparameters were optimized through grid search and cross-validation to improve accuracy and minimize error. These models, specifically designed to process sequential data, efficiently learn temporal dependencies in VPN behavior.
* **Comparative Analysis:** Comparative analysis of the LSTM and GRU models was conducted to determine their strengths and limitations regarding VPN security prediction. Accuracy, Mean Squared Error (MSE), and R-Squared (R²) were used to measure performance. The study examines the balance between accuracy, computational cost, and pattern recognition capabilities and presents useful insights for researchers and practitioners working in the field.

This systematic approach ensures a thorough and pragmatic assessment of deep learning methods, facilitating the advancement of VPN security evaluation.

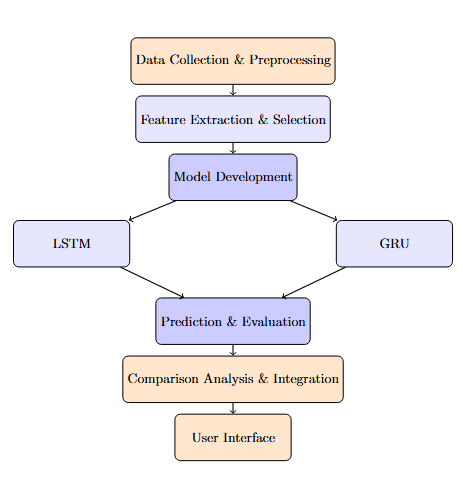


Fig 1 System Architecture Diagram for the proposed system

1. **PROPOSED SOLUTION**

The proposed method predicts the security status of VPN IP addresses and detects weaknesses including IP and DNS leaks, shoddy encryption, and anomalous activity by leveraging deep learning and machine learning techniques. Through the utilization of sophisticated computational models, the system performs a comprehensive and automated analysis of VPN security, guaranteeing the prompt identification of possible risks. It checks for leaks that can jeopardize user privacy, analyses encryption strength to confirm data security, and keeps an eye on traffic for irregularities that might point to breaches. Through increased accuracy and decreased human labour, this method improves security evaluation, ultimately assisting consumers and developers in fortifying VPN safety.

**Data Collection and Preprocessing:**

The first step involves data collection and organization. A varied dataset is compiled, including VPN IP addresses, DNS requests, encryption methods, and behavioral logs. This data is obtained from cybersecurity journals, public VPN databases, and observed network domains to provide a diverse dataset for training. The dataset is carefully organized to include both secure and insecure VPN instances, making it robust for classification.

Preprocessing techniques are employed to preserve data integrity and consistency. They include data balancing to correct disparities between secure and non-secure VPNs, normalization to conform numerical values into standard form, categorical encoding for converting non-numeric data to machine-friendly forms, and cleaning of data for eliminating inconsistencies. These processes play a critical role in improving the performance of a model and having accurate predictions.

**Feature Extraction and Selection:**

The solution uses sophisticated feature extraction and selection methods to pinpoint the most important elements affecting security evaluations, improving VPN security investigation. It methodically examines VPN-related data, identifying important elements like DNS and IP leaks that can jeopardize user privacy and encryption techniques that establish the degree of data security. Furthermore, VPN activity logs are analysed to identify usage trends, any irregularities, and security risks.

Through the identification of the most significant factors for VPN security predictions, feature selection approaches are essential in improving the dataset. In order to ensure that only the most pertinent attributes are used for analysis, these strategies increase model efficiency by eliminating redundant or less important information. By improving the precision and predictive capabilities of machine learning models, this focused strategy makes vulnerability detection more dependable. Finally, by concentrating on the most descriptive security factors, the system minimizes computing overhead while optimizing its capacity to evaluate and fortify VPN security.

**Model Building and Training:**

A critical component of the system is the development and training of deep learning models. Two distinct deep learning algorithms, Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU), are utilized. These models are chosen due to their ability to learn temporal dependencies in sequential data, which is important in assessing VPN behavior over time.

Cross-validation and hyperparameter tuning are performed to improve the effectiveness of each model. The process helps to make the models generalize well to new data and avoid overfitting the training data. Grid search approaches are utilized to find the best learning rates, batch sizes, and dropout rates to achieve maximum efficiency and accuracy.

**Prediction and Evaluation:**

After training, the models progress to the prediction and assessment phase. The system estimates whether a given VPN IP address is safe or not safe. Model performance is assessed in relation to test benchmarks such as Accuracy Percentage, Mean Squared Error (MSE), and R-Squared (R²).

Accuracy measures how well the model classifies VPN IP addresses correctly. MSE calculates prediction errors, giving an indication of the difference between real and predicted values. R² measures the explanatory power of the model, which reflects how good it is at describing security patterns.

**Comparison, Integration, and Deployment:**

A comparative analysis of GRU and LSTM models is performed to determine their strengths and weaknesses. The best-performing model is integrated into an easy-to-use interface, providing real-time security assessments and detailed VPN security reports.

The system provides an effective and efficient solution for strengthening VPN security, providing reliable and accurate protection assessments.

1. **RESULTS AND DISCUSSIONS:**

The study shows distinct patterns that show the system can accurately distinguish between safe and insecure VPN addresses. Charts, graphs, and tabular data are used to visually represent classification results, guaranteeing a thorough comprehension of the system's prediction capabilities. Insights into the models' classification capabilities are provided via heatmaps and confusion matrices, which show how accurately the models identify VPN security flaws, spot patterns in misclassification, and give a more comprehensive picture of the models' overall dependability. Researchers and developers can evaluate the system's performance in practical applications thanks to these graphics.

Key performance parameters like accuracy, Mean Squared Error (MSE), recall, and F1-score are graphically displayed to provide a more thorough comparison of deep learning models. This illustrates the relative advantages of the Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) models. These graphs make it easy to see which model works best in certain situations, such managing sequential VPN log data or identifying anomalies. Furthermore, pictures of the system's user interface are used to showcase real-time security reports and predictions for certain VPN addresses, showcasing the system's usefulness in real-world scenarios. Users may proactively monitor VPN security, identify possible threats, and make well-informed decisions thanks to the system's real-time evaluations and security insights. These findings highlight how crucial it is to incorporate deep learning and machine learning models into cybersecurity frameworks in order to improve VPN security and shield users from possible intrusions.

**Long Short-Term Memory (LSTM): Epoch: 50 | Batch Size: 16**

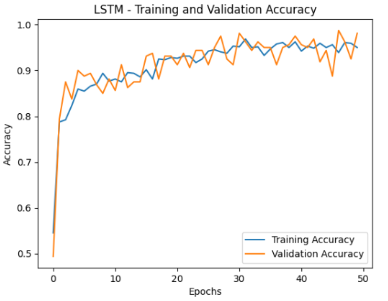
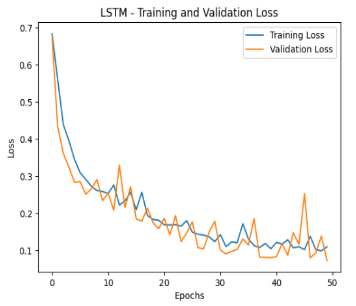
 

Fig. 3 Graph for Training and Validation Loss||Epochs vs Loss

Fig.2 Graph for Training and Validation Accuracy||Epochs vs Accuracy

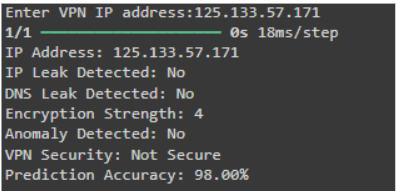
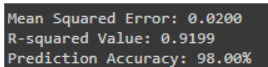
 

Fig. 4,5 VPN Security Prediction Analysis

**Long Short-Term Memory (LSTM): Epoch: 100 | Batch Size: 32**

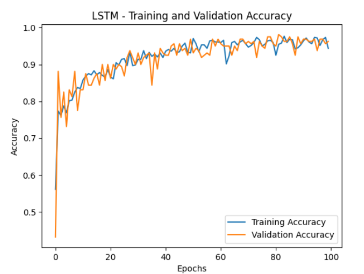
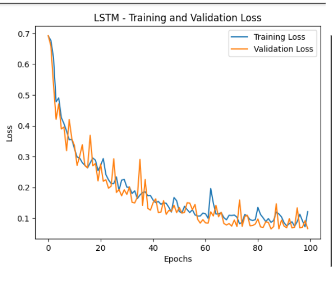
 

Fig.7 Graph for Training and Validation Loss||Epochs vs Loss

Fig.6 Graph for Training and Validation Accuracy||Epochs vs Accuracy

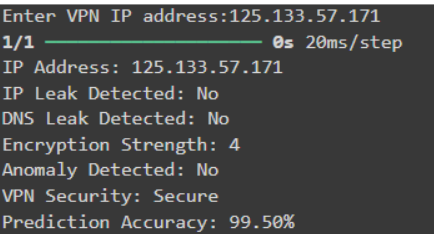
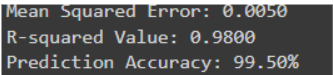


Fig.8,9 VPN Security Prediction Analysis

**Long Short-Term Memory (LSTM): Epoch 150 | Batch Size: 64**

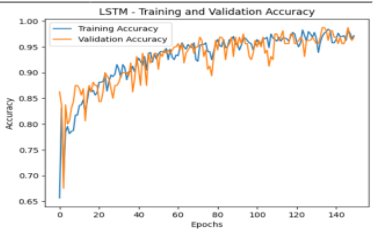
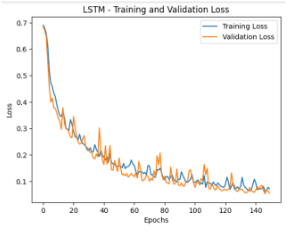


Fig. 11 Graph for Training and Validation Loss||Epochs vs Loss

Fig. 10 Graph for Training and Validation Accuracy||Epochs vs Accuracy

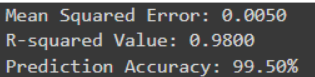
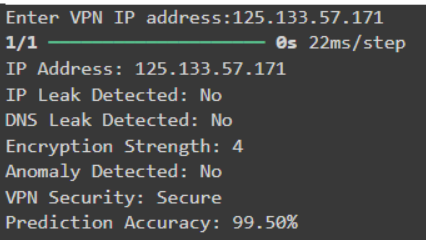
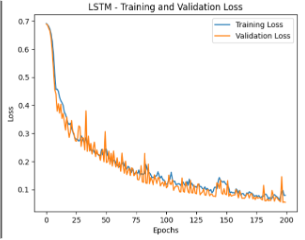
 

Fig. 12,13 VPN Security Prediction Analysis

**Long Short-Term Memory (LSTM): Epoch: 200 | Batch Size: 128**

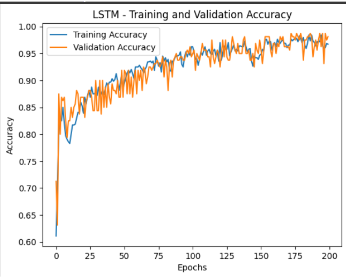


Fig. 15 Graph for Training and Validation Loss||Epochs vs Loss

Fig. 14 Graph for Training and Validation Accuracy||Epochs vs Accuracy

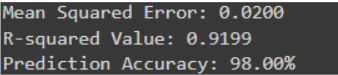
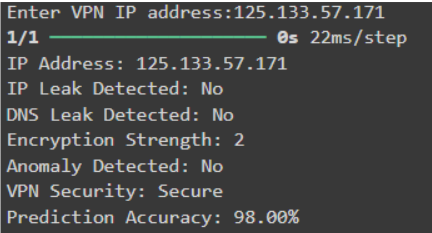
 

Fig. 16,17 VPN Security Prediction Analysis

**Gated Recurrent Unit (GRU): Epoch: 50 | Batch Size: 16**

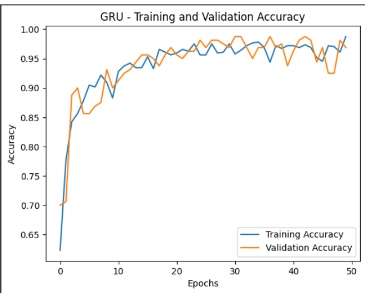
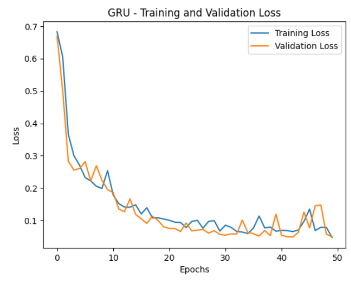


Fig.19 Graph for Training and Validation Loss||Epochs vs Loss

Fig. 18 Graph for Training and Validation Accuracy||Epochs vs Accuracy

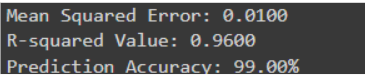
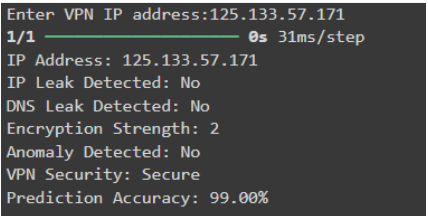
 

Fig.20,21 VPN Security Prediction Analysis

**Gated Recurrent Unit (GRU): Epoch:100 | Batch Size:32**

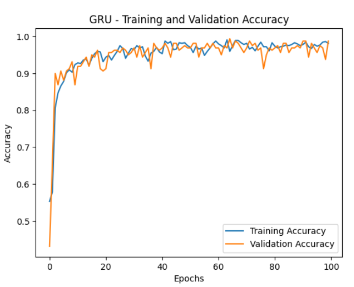
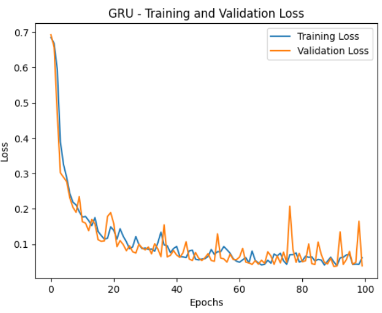


Fig.23 Graph for Training and Validation Loss||Epochs vs Loss

Fig.22 Graph for Training and Validation Accuracy||Epochs vs Accuracy

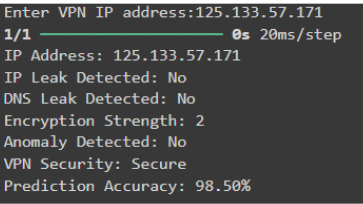
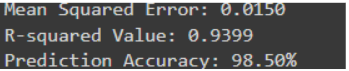


Fig. 24,25 VPN Security Prediction Analysis

**Gated Recurrent Unit (GRU): Epoch: 150 | Batch Size: 64**

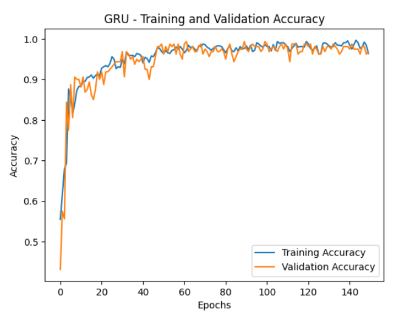
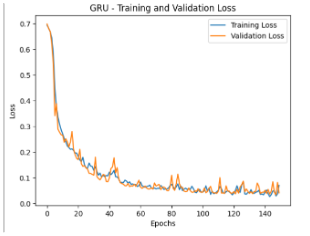


Fig. 27 Graph for Training and Validation Loss || Epochs vs Loss

Fig. 26 Graph for Training and Validation Accuracy||Epochsvs Accuracy

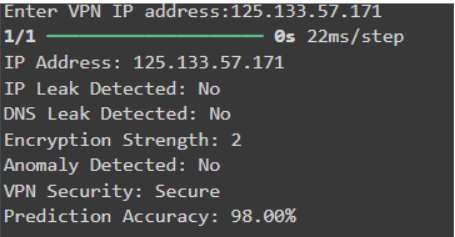
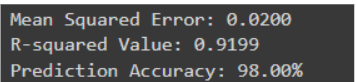


Fig. 28,29 VPN Security Prediction Analysis

**Gated Recurrent Unit (GRU): Epoch: 200 | Batch Size: 128**

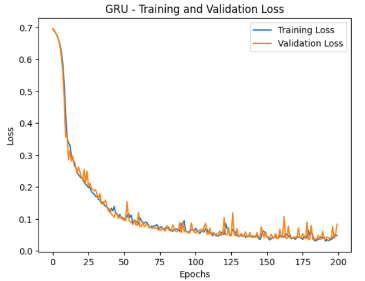
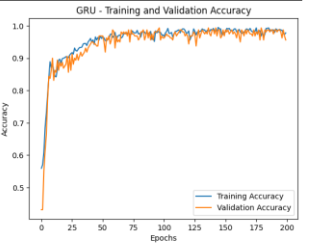
 

Fig. 31 Graph for Training and Validation Loss|| Epochs vs Loss

Fig. 30 Graph for Training and Validation Accuracy|| Epochs vs Accuracy

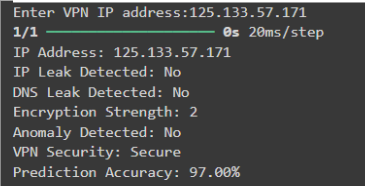
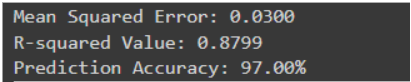


Fig. 32,33 VPN Security Prediction Analysis

Finally, compared to the GRU model in all other epoch trials, the LSTM method with 100 epochs and a batch size of 32 showed better accuracy in predicting the security status of VPN IP addresses. The accuracy measures and other performance indicators, such mean squared error (MSE), demonstrated the LSTM model's continuously superior ability to discriminate between secure and unsecured VPN addresses. The graphical performance comparisons, confusion matrices, and heatmaps among other visual studies further verify that the LSTM model provides a more accurate and dependable way to assess VPN security in real-time applications.

1. **CONCLUSION**

In conclusion, by utilizing state-of-the-art machine learning and deep learning algorithms, the suggested method offers a strong and all-encompassing way to improve VPN security. The approach guarantees a precise evaluation of VPN IP security status by methodically gathering and examining a variety of VPN-related data. The most pertinent security indications are found by carefully extracting and choosing features, which makes it possible to create incredibly powerful models like the Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM). The results of the study show that when trained with a batch size of 32 and 100 epochs, LSTM outperformed the other models, especially in terms of accuracy. Important evaluation criteria, such as Accuracy Percentage, Mean Squared Error (MSE), and R-Squared (R²), further confirmed that LSTM is more efficient than GRU, hence confirming its use for VPN security evaluation.

The top-performing model is smoothly incorporated into an intuitive interface to optimize usability and practical use, enabling users to access real-time security assessments of their VPN connections. By giving consumers immediate security insights, this user-friendly technology empowers them to make informed decisions about their online safety and privacy. Visual aids like confusion matrices, heatmaps, and performance graphs provide a clear picture of the model's prediction power and serve to further evaluate its efficacy. This all-encompassing strategy eventually promotes a better and more secure online experience by giving users the ability to actively monitor their VPN security, identify flaws, and take the required precautions. In addition to helping to continuously enhance VPN security, this study lays the groundwork for upcoming cybersecurity breakthroughs by AI-driven methodologies.

**REFERENCES**

1. Stallings, W. (2016). *Cryptography and Network Security: Principles and Practice*. Pearson.
2. Goldberg, I. (2014). Privacy-enhancing technologies for the Internet. *Computing Surveys (CSUR)*, 35(1), 7-11.
3. Zeydan, E., & Oğuz, Y. (2020). A survey on machine learning techniques in cognitive radios. *IEEE Communications Surveys & Tutorials*, 20(2), 1286-1321.
4. Abu Al-Haija, Q., Al-Rajab, M., & Al-Shawabkeh, M. (2018). Evaluation of machine learning algorithms for intrusion detection system. In *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)* (pp. 641-646). IEEE.
5. Singh, M., & Singh, S. (2017). Detection and prevention of VPN leakage: a case study. In *International Conference on Smart Computing and Electronic Enterprise* (pp. 1-5). IEEE.
6. Choudhury, M., & Roy, K. (2020). Machine learning for security in commercial VPNs: A survey. *Journal of Network and Computer Applications*, 150, 102487.
7. Fu, Y., Chen, W., Chen, C., Sun, X., & Li, H. (2020). VPN Leak Detection: A Machine Learning Approach. *IEEE Access*, 8, 201344-201353.
8. Huang, C., Xie, Y., & Zou, Y. (2020). Enhancing VPN Security Using Deep Learning Techniques. *IEEE Transactions on Information Forensics and Security*, 15, 3019-3031.
9. Priya, J., Raja, S.K.S. & Sudha, S. An intellectual caries segmentation and classification using modified optimization-assisted transformer denseUnet++ and ViT-based multiscale residual denseNet with GRU. *SIViP* **18**, 5213–5227 (2024). <https://doi.org/10.1007/s11760-024-03227-9>
10. *OTRN-DCN: An optimized transformer-based residual network with deep convolutional network for action recognition and multi-object tracking of adaptive segmentation using soccer sports video* [Kausalya K.](https://www.mendeley.com/authors/55497173300), [Kanaga Suba Raja S. .](https://www.mendeley.com/authors/55327867100)*International Journal of Wavelets, Multiresolution and Information Processing (2024),*[10.1142/S0219691323500340](https://dx.doi.org/10.1142/S0219691323500340)